PERCEPTION POINT

Advanced Collaboration Security

Holistic threat detection for the digital-first enterprise.

Highlights.

Threat Coverage
APTs
Zero Days/N-Days
Phishing
Malware
Impersonation
BEC

Real-time prevention
Block malicious content before it ever reaches the end user.

X-ray visibility
CPU-level visibility sees code before it can be masked.

Deep scanning
Unpacks and follows URLs to detect evasive malicious intent.

One-click deployment
Easy and fast deployment on the cloud. No change to existing processes.

Unlimited scale
Scan 100% of content, regardless of volume.

Zero Delay
In-line engines work in seconds.

Cloud Collaboration Apps: A growing security blindspot across the enterprise.

The need to communicate and collaborate on a global level has created a proliferation of cloud-based tools for businesses. **Email. Cloud Storage apps. Messaging platforms. Social Networks. CRM.** As many as 20 apps in a single enterprise.

But with new channels come new gaps for hackers, and many new security blind spots.
You need full threat visibility across channels with a solution that works at the speed your company does.

OUR SOLUTION:

Agile & Unified Threat Detection For Any Channel.

We stop malicious content (files, URLs & payload-less attacks) from infiltrating your organization via any collaboration channel. Unique CPU-level visibility plus deep scanning capabilities detect the advanced attacks and evasion techniques that easily bypass legacy security technologies. In addition, multi-layered platform combines multiple threat intelligence, image recognition, static and BEC engines to prevent phishing, malware, impersonation and social engineering attacks.

Our service deploys in one-click, has virtually zero scanning delay, and limitless scale – so your employees can collaborate both securely and seamlessly, wherever they are.

Email

G Suite
Exchange
Office 365

Any web-based email service

Cloud Storage

OneDrive
Dropbox
Google Drive
box
SharePoint

Cloud Collaboration

New
Salesforce
slack
Teams

API

Integration with any other application where files or URLs are exchanged.

Custom development per client needs.

Contact Us

www.perception-point.io
info@perception-point.io

We're in
Boston | Tel Aviv

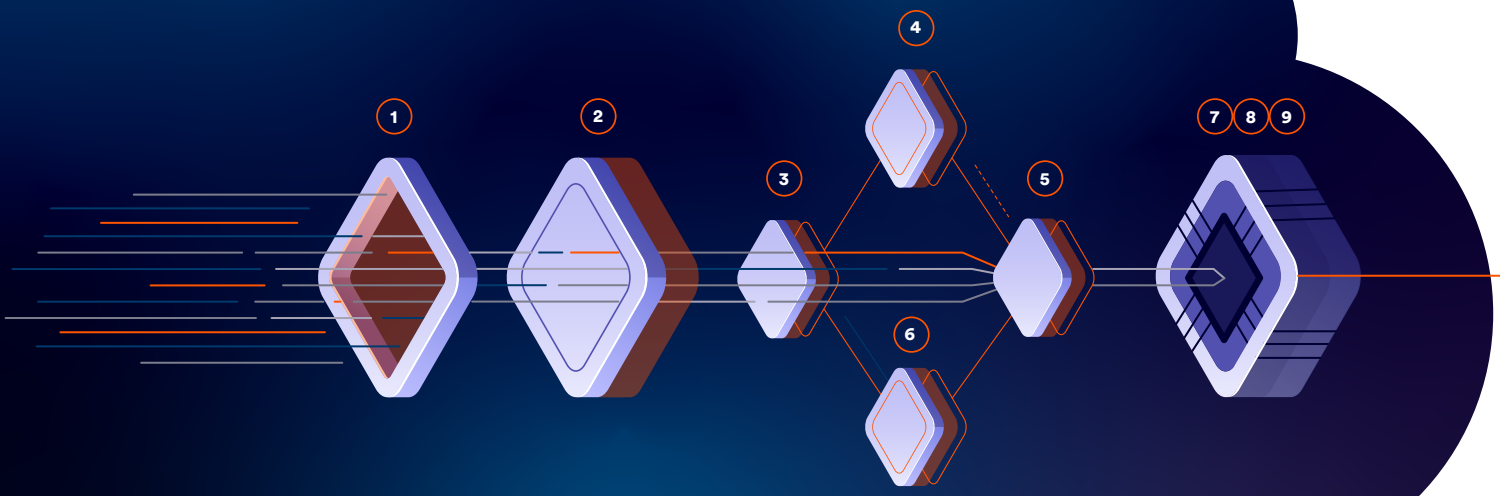
Free 30-day trial

Set-up a trial in less than an hour, with no interference or disturbance to the end user or organization.
No content will be stored and all data is encrypted.

PERCEPTION POINT

Inherent Layered Solution

Enhanced standard layers + cutting-edge APT protection for the most high-performance defense on the market.



Everyday Threats | Phishing, Malware, Impersonation, BEC, etc.

1

Spam Filter (Email Only).

Receives the email and applies reputation and anti-spam filters to quickly flag an email as malicious.

2

Recursive Unpacker.

Unpacks the content into smaller units (files and URLs) to identify hidden malicious attacks. Further extracts embedded URLs and files (recursively) by unpacking files and following URLs. All of the extracted components go separately through the next security layers.

3

Threat Intelligence.

Combines multiple threat intelligence sources with our internally devloped engine that scans URLs and files in the wild to warn about potential or current attacks.

4

Phishing Engines.

Combines best-in-class URL reputation engines and an in-house image analysis engine to identify impersonation techniques and phishing attacks.

5

Static Signatures.

Combines best-in-class signature based anti-virus engines to identify malicious attacks. In addition, we've developed a tool that acts to identify highly complicated signatures.

6

BEC

Prevention of payload-less attacks including spoofing, look-alike domain and display name deception.

N-DAY/ ZERO-DAY THREATS

First Hardware-Assisted Platform (HAP™)

Unique CPU-level technology acts earlier in the kill chain than any other solution. Blocking attacks at the exploit phase - pre-malware release - for true APT prevention.

7

HAP™ (Dropper).

Employs advanced heuristics-based engine for detecting logical bugs and handling macros and scripts.

8

HAP™ (CFG).

Records the CPU while it processes the input (files and URLs) and identifies exploits by examining the entire execution flow - detecting any deviation from the normal flow of a program in order to deterministically identify malicious activity.

9

HAP™ (FFG).

Detects advanced techniques such as exploits that are written to bypass common CFI algorithms. Proprietary semantic aware control flow graphs developed for each application identify deviations of the execution flow during runtime.

Protect multiple channels with our full Advanced Collaboration Security platform.
Email, Messaging, Cloud storage, CRM + API for any content-exchange channel

PERCEPTION POINT